

Claims

- [1] A method for requesting a service-specific traffic encryption key from a subscriber station to a base station in a wireless portable Internet system, the method comprising:
- (a) determining a service type for the requested traffic encryption key to be used for security on a traffic connection to the base station prior to establishing the traffic connection;
 - (b) generating a Key Request message for requesting a traffic encryption key corresponding to the determined service type; and
 - (c) sending the generated Key Request message to the base station using a media access control (MAC) message.
- [2] The method as claimed in claim 1, wherein the service type in the step (b) is recorded in a parameter included in the Key Request message.
- [3] The method as claimed in claim 1 or 2, wherein the service type comprises a unicast service, a multicast service, and a broadcast service.
- [4] The method as claimed in claim 3, wherein when the service type is a multicast service, the parameter of the Key Request message includes an ID containing an identifier of a multicast service group for a subscriber.
- [5] The method as claimed in claim 3, wherein the step (c) includes sending the Key Request message using a PKM-REQ (Privacy Key Management - Request) that is one of MAC messages of the IEEE 802.16 standard protocol.
- [6] A method for generating and distributing a service-specific traffic encryption key from a base station to a subscriber station in a wireless portable Internet system, the method comprising:
- (a) receiving a Key Request message from the subscriber station requesting the service-specific traffic encryption key;
 - (b) analyzing the Key Request message to determine a service type;
 - (c) generating a traffic encryption key according to the determined service type; and
 - (d) generating a Key Reply message including the generated traffic encryption key and sending the generated Key Reply message to the subscriber station using a MAC message.
- [7] The method as claimed in claim 6, wherein in the step (b), the Key Request message includes a parameter related to the service type, the base station

analyzing the parameter to determine the service type.

- [8] The method as claimed in claim 6 or 7, wherein the step (c) includes:
in the case that generation of the traffic encryption key for the subscriber station is a failure due to the determined service type, the base station generating a Key Reject message including an error code indicating a reason of the failure and sending the generated Key Reject message to the subscriber station using a MAC message.
- [9] The method as claimed in claim 8, wherein the base station enters “unsupported service type” on the error code and sends the error code to the subscriber station in the case that the traffic encryption key for a service type corresponding to a traffic encryption key request of the subscriber station cannot be generated and distributed.
- [10] The method as claimed in claim 8, wherein the service type comprises a unicast service, a multicast service, and a broadcast service.
- [11] The method as claimed in claim 10, wherein the base station enters “unauthorized multicast service group ID” on the error code and sends the error code to the subscriber station in the case that the service type for the traffic encryption key requested by the subscriber station is a multicast service and defined as unsupported multicast service for the specific multicast service group ID, because the SS is not authorized for the specific multicast service group by the base station.
- [12] The method as claimed in claim 8, wherein the Key Reply message and the Key Reject message are sent using a PKM-RSP (Privacy Key Management - Response) message that is one of MAC messages of the IEEE 802.16 standard protocol.
- [13] A protocol configuration method for generating and distributing a service-specific traffic encryption key to be used for security on a traffic connection between a base station and a subscriber station in the wireless portable Internet system, the protocol configuration method comprising:
(a) the subscriber station sending a Key Request message for requesting a service-specific traffic encryption key to the base station using a MAC message; and
(b) the base station analyzing the Key Request message received from the subscriber station, generating the requested service-specific traffic encryption key, and sending a Key Reply message including the generated service-specific

- traffic encryption key to the subscriber station using a MAC message.
- [14] The protocol configuration method as claimed in claim 13, wherein the step (a) comprises:
sending the Key Request message using a PKM-REQ message that is one of MAC messages of the IEEE 802.16 standard.
- [15] The protocol configuration method as claimed in claim 13, wherein the step (b) comprises:
sending a Key Reject message including an error code recording a reason of a failure to the subscriber station using a MAC message in the case that generation of the service-specific encryption key is failed.
- [16] The protocol configuration method as claimed in claim 15, wherein the step (b) comprises:
sending the Key Reply message and the Key Reject message using a PKM-RSP message that is one of MAC messages of the IEEE 802.16 standard protocol.
- [17] An apparatus wirelessly connected to a base station in a wireless portable Internet system so as to request a service-specific traffic encryption key from the base station, the apparatus comprising:
a Key Request message generator for generating a Key Request message for requesting the service-specific traffic encryption key from the base station;
a Key Request message sender for sending the Key Request message of the Key Request message generator to the base station using a MAC message;
a Key Reply/Reject message receiver for receiving a Key Reply message or a Key Reject message from the base station using a MAC message;
a message analyzer for analyzing the Key Reply message or the Key Reject message from the Key Reply/Reject message receiver to extract the traffic encryption key from the Key Reply message, or analyze an error type from the Key Reject message; and
a key request controller for controlling operations of the Key Request message generator, the Key Request message sender, the Key Reply/Reject message receiver, and the message analyzer, and requesting the base station to allocate the service-specific traffic encryption key and process the traffic encryption key according to the requested key allocation or an error code generated upon occurrence of an error as received from the base station.
- [18] The apparatus as claimed in claim 17, wherein the Key Request message comprises a service type and a multicast service group ID of the subscriber

station when the service type is a multicast service.

- [19] The apparatus as claimed in claim 17, further comprising:
a memory for storing information including the traffic encryption key or the error code resulted from an analysis of the message analyzer under the control of the key request controller.
- [20] An apparatus provided to a base station for generating and distributing a service-specific traffic encryption key in a wireless portable Internet system, the apparatus comprising:
a Key Request message receiver receiving a Key Request message from the subscriber station using a MAC message;
a message analyzer analyzing the Key Request message of the Key Request message receiver to extract information including a service type in the Key Request message;
a subscriber discriminator determining whether a traffic encryption key can be allocated to a requested service type according to the Key Request message;
a traffic encryption key generator generating a service-specific traffic encryption key analyzed by the message analyzer;
a Key Reply message sender generating a Key Reply message including the traffic encryption key generated by the traffic encryption key generator according to the requested service type from the subscriber station, and sending the generated Key Reply message to the subscriber station using a MAC message; and
a key generation and distribution controller for controlling operations of the Key Request message receiver, the message analyzer, the subscriber discriminator, the traffic encryption key generator, and the Key Reply message sender to generate and distribute a corresponding service-specific traffic encryption key according to a request for service-specific traffic encryption key refreshment from the subscriber station.
- [21] The apparatus as claimed in claim 20, further comprising:
a Key Reject message sender for sending a Key Reject message including an error code to the subscriber station using a MAC message under the control of the key generation and distribution controller in the case that the traffic encryption key generator generates an error for the request of the subscriber station.
- [22] The apparatus as claimed in claim 20, further comprising:

a memory for storing information including an analysis result of the message analyzer and a discrimination result of the subscriber discriminator under the control of the key generation and distribution controller.